MEMORY CARD

Patent number: JP2003288564

Publication date: 2003-10-10

Inventor: NAKABE FUTOSHI; MASAKI TADAKATSU; KAWANO SHINJI; OZEKI HIDEO; EBARA HIROMI

Applicant: MATSUSHITA ELECTRIC IND CO LTD

Classification:

- international: ***G06F12/14; G06K19/00; G06K19/073;*** **G06F12/14; G06K19/00; G06K19/073;** (IPC1-7): G06K19/073; G06F12/14; G06K19/00

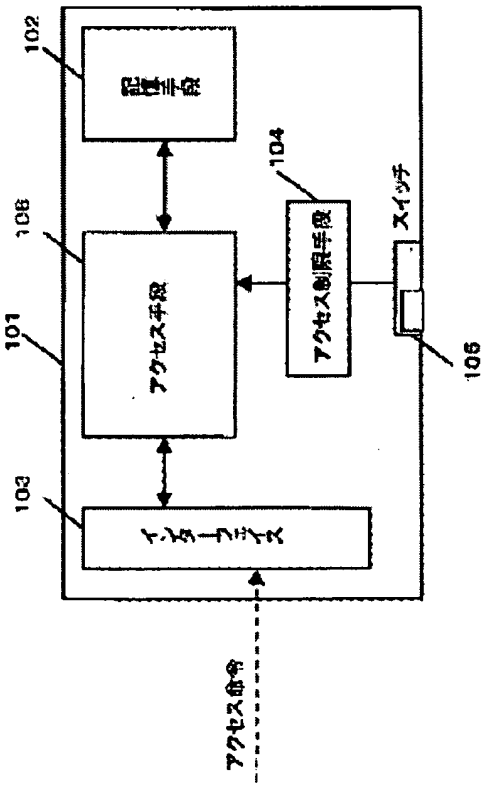
- european:

Application number: JP20030006553 20030115

Priority number(s): JP20030006553 20030115; JP20020015008 20020124

Abstract of **JP2003288564**

PROBLEM TO BE SOLVED: To provide a memory card which has reliable security by a simple mechanism.
SOLUTION: The memory card receives an access instruction from external connection equipment to a storage means and accesses the storage means by an access means according to the access instruction, and a switch constituting the memory card shows whether the storage means can be accessed. An access limiting means limits the access to the storage means by the access means according to the state of the switch.
COPYRIGHT: (C)2004,JPO



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－288564
（P2003－288564A）
(43)公開日　平成15年10月10日(2003.10.10)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｋ　19/073		Ｃ０６Ｆ　12/14	３１０Ｂ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３１０	Ｃ０６Ｋ　19/00	Ｐ	５Ｂ０３５
Ｇ０６Ｋ　19/00			Ｑ	

審査請求　未請求　請求項の数12　ＯＬ　（全 11 頁）

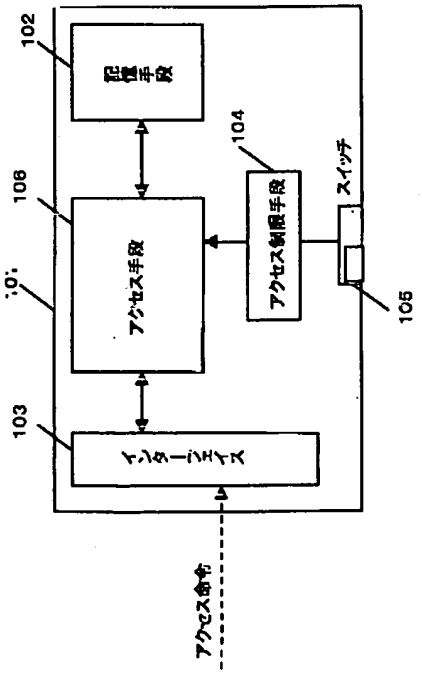
(21)出願番号　特願2003－6553(P2003－6553)
(22)出願日　平成15年１月15日(2003.1.15)
(31)優先権主張番号　特願2002－15008(P2002－15008)
(32)優先日　平成14年１月24日(2002.1.24)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　中部　太志
東広島市鏡山３丁目10番18号　株式会社松下電器情報システム広島研究所内
(72)発明者　正木　忠勝
東広島市鏡山３丁目10番18号　株式会社松下電器情報システム広島研究所内
(74)代理人　100083172
弁理士　福井　豊明

最終頁に続く

(54)【発明の名称】　メモリカード

(57)【要約】
【課題】　簡便な仕組みにより確実なセキュリティを有するメモリカードを提供する。
【解決手段】　外部接続機器からの記憶手段へのアクセス命令を受信し、当該アクセス命令に応じてアクセス手段が記憶手段へのアクセスを行うメモリカードにおいて、メモリカードを構成するスイッチは、記憶手段へのアクセスの可否を示す。また、アクセス制限手段は、スイッチの状態に基づいて上記アクセス手段の上記記憶手段へのアクセスを制限する。



【特許請求の範囲】
【請求項１】　外部接続機器からの記憶手段へのアクセス命令を受信し、当該アクセス命令に応じてアクセス手段が上記記憶手段へのアクセスを行うメモリカードにおいて、
上記記憶手段へのアクセスの可否を示すスイッチと、
上記スイッチの状態に基づいて上記アクセス手段の上記記憶手段へのアクセスを制限するアクセス制限手段と、
を具備することを特徴とするメモリカード。
【請求項２】　上記記憶手段は、アクセスするための認証が必要な領域と不要な領域とを備え、
上記アクセス制限手段は、上記スイッチの状態に基づいて上記アクセス手段の上記認証が必要な領域へのアクセスを制限する請求項１に記載のメモリカード。
【請求項３】　上記アクセス手段は、上記認証が必要な領域にアクセスするための認証を行い当該認証の結果に応じて上記認証の必要な領域にアクセスするに際して、
上記アクセス制限手段は、上記認証の必要な領域へのアクセスを制限する請求項２に記載のメモリカード。
【請求項４】　上記記憶手段は、電子商取引にて利用される領域を備え、
上記アクセス手段は、上記アクセス命令が電子商取引に関する命令か否かを判断し、当該アクセス命令が電子商取引に関する命令である場合には上記領域にアクセスするに際して、
上記アクセス制限手段は、上記電子商取引にて利用される領域へのアクセスを制限する請求項１に記載のメモリカード。
【請求項５】　上記電子商取引にて利用される領域は、ＴＲＭ（Tamper Resist Module）内に具備される請求項４に記載のメモリカード。
【請求項６】　上記記憶手段へのアクセスは、上記記憶手段からのデータの読み出しである請求項１に記載のメモリカード。
【請求項７】　上記記憶手段へのアクセスは、上記記憶手段へのデータの書き込みである請求項１に記載のメモリカード。
【請求項８】　上記スイッチは、ハードウェアで構成される物理スイッチである請求項１に記載のメモリカード。
【請求項９】　挿入部位を上記外部接続機器の所定のスロットに挿入する構成である場合に、
上記スイッチは、挿入部位に設けられる請求項８に記載のメモリカード。
【請求項１０】　挿入部位を上記外部接続機器の所定のスロットに挿入する構成である場合に、
上記スイッチは、非挿入部位に設けられる請求項８に記載のメモリカード。
【請求項１１】　さらに、上記アクセス制限手段は、所定のタイミングで上記スイッチの状態を検知して当該状態を状態記憶手段に記憶すると共に、上記状態の変更に基づいて上記アクセス手段の上記記憶手段へのアクセスを禁止する請求項１に記載のメモリカード。
【請求項１２】　上記アクセス制限手段は、上記外部接続機器にパスワードを要求すると共に該外部接続機器から入力されたパスワードと予め内部にて記憶したパスワードとに基づいて上記アクセスの禁止を解除する請求項１１に記載のメモリカード。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、メモリカードに関し、特に、セキュリティ機能を有するメモリカードに関する。
【０００２】
【従来の技術】近年、例えば不揮発性メモリを備えたメモリカードの小型化、大容量化が目覚しく、ゆえに様々な分野での応用が期待されている。
【０００３】例えばメモリカードの小型化により様々な機器への装着が可能となるばかりでなく、大容量化により記憶すべきデータ量の多い機器への使用も可能になっている。また、メモリカードに共通の仕様を与えることにより１つのメモリカードを複数の機器にて使用することも可能である。
【０００４】また、上記メモリカードの利用が期待される機器においても様々な変化が起こっている。即ち、ＪＡＶＡ（登録商標）等のプラットホームを選ばない言語を用いることによる各機器の制御の共通化や、ネットワーク接続によって遠隔操作、情報共有等を可能にする点等である。
【０００５】ところで、上記メモリカードへの書き込みを保護する技術として、特開２０００－９９６７６号公報に記載の技術がある。当該公報には、メモリカードに、当該メモリカードへのデータの書き込みを禁止する設定を行うスイッチを設け、制御装置（ここではホストコンピュータ）からの命令（ここでは問い合わせ）に対して、メモリカードに設けられた制御手段が上記スイッチの設定状態を上記制御装置に送信する技術が記載されている。
【０００６】上記技術では、上記スイッチの設定内容に応じて、上記制御装置がデータの書き込み禁止の処理を行うことができるとしている。
【０００７】
【特許文献１】特開２０００－９９６７６号公報
【０００８】
【発明が解決しようとする課題】上述したように、小型化、大容量化により様々な分野に応用が期待されているメモリカードであるが、様々な分野に適応可能にするがゆえにセキュリティが必要である。特にプライベート情報や電子商取引に必要な情報等、取り扱いに細心の注意が必要な情報の記憶に利用されるメモリカードには強固

なセキュリティを備えることが求められる。また、当該メモリカードを利用する機器が善意の使用とは限らないため、当該機器との連携ではなくメモリカードのみでセキュリティを備える必要がある。

【0009】しかしながら、上記特開2000-99676号公報に記載の技術は、例えばユーザの誤操作によってデータが消去されるのを防止するための技術であり、メモリカード自体がセキュリティを備えているとはいえない。

【0010】即ち、上記特開2000-99676号公報に記載されたメモリカードは、例えば携帯電話等の制御装置に対してスイッチがオンかオフかの情報を通知するだけである。このため、上記制御装置が悪意を持って制御されている場合には、当該オンやオフといった情報を無視して、又はオンやオフといった問い合わせを行わずにメモリカードにデータを書き込むことが可能である。また、メモリカードに記憶されているデータの読み出しに関しては上記スイッチはまったく機能しておらず、なんら障害なしにデータを読み出すことが可能である。従来より汎用的に用いられているフロッピーディスク（R）においても同様のことが言える。

【0011】また、従来では例えばメモリカードが盗難に遭い、さらに悪意を持った人によりデータを読み出されない限り、メモリカードに記憶されているデータは安全であると言えた。

【0012】しかしながら昨今では、上述したように、プラットホームを選ばない言語が用いられつつあるため、当該言語を利用した悪意あるプログラムを（制御）機器に実行させることが可能である。さらに、各機器がネットワークに接続されて利用されつつあるため、上記悪意あるプログラムを上記（制御）機器に何らかの方法でダウンロード及び実行させ、実行された当該悪意あるプログラムがメモリカードからデータを読み出し、ネットワークを通じて送信することが可能となる。事実、コンピュータウイルスに同様の動作を行うものが存在することは多数報告されている。さらに、特に上記メモリカードが非接触ＩＣカードのように無線通信にてアクセスされる場合には、ユーザが全く気付かないうちにメモリカードにアクセスされることもありうる。

【0013】このような状況においては、ユーザが手元にメモリカードを持っているにもかかわらず、ユーザが気付かないうちに当該メモリカードに記憶しているデータが読み出され、又は改変されるということが十分に起こりうるのである。

【0014】本発明は、上記従来の事情に基づいて提案されたものであって、簡便な仕組みにより、確実なセキュリティを有するメモリカードを提供することを目的とする。

【0015】

【課題を解決するための手段】本発明は、上記目的を達成するために以下の手段を採用している。即ち、本発明は、外部接続機器からの記憶手段へのアクセス命令を受信し、当該アクセス命令に応じてアクセス手段が記憶手段へのアクセスを行うメモリカードを前提としている。ここで、メモリカードを構成するスイッチは、記憶手段へのアクセスの可否を示す。また、アクセス制限手段は、スイッチの状態に基づいて上記アクセス手段の上記記憶手段へのアクセスを制限する。

【0016】以上のように、メモリカード自身がスイッチの状態を判断し、さらにメモリカード自身が記憶手段へのアクセスを制限することで、例えば外部接続機器が悪意をもって記憶手段にアクセスした場合であっても、外部接続機器に依存することなくスイッチの状態に基づいて確実にアクセスを制限することが可能になる。

【0017】また、上記記憶手段は、アクセスするための認証が必要な領域と不要な領域とを備える場合には、アクセス制限手段は、スイッチの状態に基づいてアクセス手段の上記認証が必要な領域へのアクセスを制限する構成がある。

【0018】さらに、アクセス手段が認証が必要な領域にアクセスするための認証を行い当該認証の結果に応じて上記認証の必要な領域にアクセスする構成でもよい。

【0019】またさらに、記憶手段は電子商取引にて利用される領域を備える場合であって、アクセス手段が、アクセス命令が電子商取引に関する命令か否かを判断し当該アクセス命令が電子商取引に関する命令である場合には上記領域にアクセスする場合には、アクセス制限手段は、上記電子商取引にて利用される領域へのアクセスを制限する構成としてもよい。

【0020】上記構成では、適所のアクセスを制限する事により、認証を必要とする領域と必要としない領域、或いは電子商取引に使用する領域とそれ以外の領域とを独立してアクセス制限する事が可能になる。従って、汎用メモリ部は利用可能としながらも、セキュアメモリ部へのアクセスを確実に防ぐといった区別ができ、即ちユーザはメモリカードの利便性を損なうことなく情報の安全性を手に入れる事ができる。尚、電子商取引にて利用される予め決められた記憶手段は、ＴＲＭ（Tamper Resist Module）内に具備される記憶手段とすることができる。

【0021】また、記憶手段へのアクセスは、記憶手段からのデータの読み出しとする構成や記憶手段へのデータの書き込みが挙げられる。

【0022】さらにまた、上記スイッチを物理スイッチとし、当該メモリカードのアクセス時に挿入部位を外部接続機器の所定のスロットに挿入する構成である場合に、スイッチを挿入部位に設ける構成がある。

【0023】この構成では、メモリカードを外部接続機器から抜くまではスイッチを操作できないため、意図せぬスイッチの操作（オン・オフ）を防止することができ

る。

【0024】また、スイッチを非挿入部位に設ける構成がある。

【0025】この構成では、メモリカードを外部接続機器から抜くことなくスイッチの操作が可能となり、随時スイッチの操作を可能とすることができる。

【0026】さらに、アクセス制限手段は、スイッチの状態を検知して状態記憶手段に記憶すると共に、状態の変更に基づいてアクセス手段の記憶手段へのアクセスを禁止する構成としても良い。

【0027】この構成では、例えばスイッチがオフの状態でメモリカードを紛失した場合、スイッチをオンにするのみでは記憶手段にアクセスできないため、メモリカードを紛失した場合などのアクセス制限（セキュリティ）も期待できる。

【0028】尚、アクセス制限を解除する方法として、アクセス制限手段が外部接続機器にパスワードを要求すると共に該外部接続機器から入力されたパスワードと予め内部にて記憶したパスワードとに基づいてアクセスの禁止を解除する構成とすることができる。

【0029】この構成では、スイッチの状態が変更された場合のみパスワードが要求されるため、例えば電子商取引を複数回連続して行った場合等では、ユーザが連続してパスワードを入力するといった手間を省くことができる。

【0030】

【発明の実施の形態】以下、添付図面を参照して、本発明の実施の形態につき説明し、本発明の理解に供する。尚、以下の実施の形態は、本発明を具体化した一例であって、本発明の技術的範囲を限定する性格のものではない。

（実施の形態１）図1は、本発明に係るメモリカードの、実施の形態１における概略機能ブロック図であり、図2は、上記メモリカードのハードウェアの概略図、図3は外部接続機器にメモリカードを挿入した際のイメージ図である。

【0031】当該メモリカード１０１は、例えば切手サイズで厚さ２ｍｍ程度の板状の構成を有し、外部接続機器３０１に挿入し又は組み込むことで、当該外部接続機器３０１はメモリカード１０１を利用することができる。尚、上記外部接続機器３０１は、例えば携帯電話であり、ユーザは当該携帯電話の通信機能を利用して電子商取引可能な所定のウェブサイトに接続し、取引を行うことが一例として挙げられる。上記例では、上記携帯電話は上記メモリカード１０１の記憶手段１０２に記憶された電子マネー等の様々な情報を用いて電子商取引を行うことになる。

【0032】上記メモリカード１０１を使用する際には、外部接続機器３０１のスロット３０２に対して当該メモリカードの挿入部位３０３を内設させることにより、メモリカードのインターフェイス１０３（図３：３０４）と上記外部接続機器３０１の内蔵インターフェイス（図示せず）が通信可能に接続される。

【0033】上記メモリカード１０１のインターフェイス１０３と外部接続機器３０１の内蔵インターフェイスとが接続されると、上記外部接続機器３０１は当該インターフェイス１０３を介して、メモリカード１０１にアクセス命令やデータ等を送信可能となり、またメモリカード１０１自身が電源を持たない場合には必要に応じて電源を供給可能となる。さらに、上記メモリカード１０１には、例えばユーザが指等でスライド可能な物理スイッチであるスイッチ１０５が設けられており、ユーザが任意にスイッチ１０５をオン・オフすることが可能になっているが詳細は後述する。

【0034】次に、図２Ａを用いて、上記メモリカード１０１のハードウェア構成について説明する。尚、理解に供するため、不要な部分を除き本発明に関連する部分のみ説明する。

【0035】上記メモリカード１０１は、ハードウェアとしてインターフェイス２０１を備え、該インターフェイス２０１は、ＣＰＵ（Central Processing Unit）２０２と接続されている。また、該ＣＰＵ２０２は、不揮発性メモリ等で構成される記憶手段２０３と例えば3つのラインで接続されている。3つのラインとは、それぞれデータライン２０４、アドレスライン２０５、及び制御ライン２０６である。上記データライン２０４は、記憶手段２０３にデータを書き込む際、又は読み出す際にデータが送受信されるラインであり、上記アドレスライン２０５は、上記データの読み出しや書き込みの際に、対象となるデータが記憶されている記憶手段２０３上のアドレスが送信されるラインである。また、上記制御ライン２０６は、上記記憶手段２０３への命令、即ち書き込み命令や読み出し命令が送信される。また、上記ＣＰＵ２０２にはスイッチ２０７と直接連動するラインが入力されており、上記スイッチ２０７が“オン”の場合には、所定の電圧（例えば３．３Ｖ）が上記ＣＰＵ２０２に入力される構成となっている。尚、この構成では、当該ＣＰＵ２０２が図１にて示すアクセス手段１０６に該当し、スイッチ２０７がスイッチ及びアクセス制限手段に該当する。

【0036】続いて、外部接続機器３０１からの記憶手段１０２へのアクセス手順を説明する。例えば、上記外部接続機器３０１が上記記憶手段１０２に記憶されている情報であるデータを読み出そうとする場合、上記外部接続機器３０１は、上記インターフェイス１０３を介してメモリカード１０１のアクセス手段１０６に読み出し命令を送信する。

【0037】当該読み出し命令を受信したアクセス手段１０６は、上記記憶手段１０２（２０３）から所定のデータを読み出す前に、アクセス制限手段１０４を介して

スイッチ１０５の状態を判断する。

【００３８】ここで、上記スイッチ１０５（２０７）の状態が例えば“オン”であれば、上記記憶手段１０２（２０３）へのアクセスが許可されているため、上記アクセス手段１０６は、当該記憶手段１０２（２０３）から目的とするデータを読み出した後、インターフェイス１０３（２０１）を介して上記外部接続機器３０１に送信する。上記スイッチ１０５（２０７）の状態は、例えば“オン”の状態ではＣＰＵ２０２の、所定のラインの電圧がハイレベルになっていることで判断可能である。尚、この構成では、上記アクセス手段１０６は例えばＣＰＵ２０２にて実行されるプログラムであり、アクセス制限手段１０４はＣＰＵ２０２に入力される所定のライン及び当該ラインの電圧を判断するプログラムとして提供される。また、スイッチ１０５はハードウェアで構成されるスイッチ、即ち物理スイッチである。

【００３９】以上のように、メモリカード自身がスイッチの状態を判断し、さらにメモリカード自身が記憶手段へのアクセスを制限することで、例えば外部接続機器が悪意をもって記憶手段へのアクセスを試みた場合であっても、当該外部接続機器に依存することなくスイッチの状態に基づいて確実にアクセスを制限することが可能になる。当該アクセス制限は、近年増加しつつある、ネットワーク機能を利用した、悪意を持った外部からのアクセスを確実に防止することが可能となる。また、ユーザが物理的にスイッチをオン・オフする構成とすることで、ユーザが気付かないうちに当該メモリカードに記憶しているデータが読み出されるという事態を、メモリカードを外すことなく防止できるため、利便性を高めると共にユーザに安心感を与えることが可能になる。

【００４０】尚、上記外部接続機器３０１からの命令が読み出し命令の場合を説明したが、当該スイッチを利用して書き込み命令も同様に防止することができる。このため、従来の、ユーザの誤操作による書き込み防止機能に加えて、記憶手段に記憶されているデータの外部からの改変をも防ぐことが可能になる。

【００４１】また、上記図２Ａに示したメモリカードの構成の他に、図２Ｂに示した構成としても良い。即ち、スイッチ２０７を、例えば制御ライン２０６に接続されるＡＮＤ回路２０９に接続するのである。この構成では、スイッチ２０７が“オン”の場合しかＣＰＵ２０２からの制御信号は記憶手段２０３に送信されないため、上記図２Ａの場合と同様の効果を有する。さらに、スイッチ２０７の状態の判断にプログラムが全く関与しないため、悪意を持つ者がネットワーク等を利用してメモリカード内のプログラムを改変した場合でも記憶手段へのアクセスを確実に制限することができる。当然、非接触ＩＣカードなどにて利用される無線通信でも同様に記憶手段へのアクセスを確実に制限する事ができる。さらに、非接触／接触ＩＦをもつＩＣカード（コンビＩＣカード）においても、同様の記憶手段へのアクセスを確実に制限可能である。尚、この構成では、ＡＮＤ回路２０６がアクセス制限手段１０４を構成するが回路をＡＮＤ回路に限定する必要は無く、物理的に記憶手段へのアクセスを制限するものであればよい。

【００４２】また、上記メモリカード１０１の挿入部位３０３に上記スイッチ１０５を設けることで、メモリカードを外部接続機器から抜くまでは当該スイッチを操作できないため、意図せぬスイッチの操作（オン・オフ）を防止することができる。

【００４３】また、上記メモリカード１０１の挿入部位３０３以外、即ち非挿入部位３０４に上記スイッチ１０５を設けることで、メモリカードを外部接続機器から抜くことなくスイッチの操作が可能となり、随時スイッチの操作を可能とすることができる。

（実施の形態２）続いて、上記スイッチが変更されたことを検出する仕組みを備えたメモリカードについて説明する。図４は、本実施の形態２におけるメモリカードの概略機能ブロック図であり、以下その構成を上記と異なる点のみ説明する。

【００４４】本実施の形態２におけるメモリカード４０１は、上記メモリカード１０１の構成に加えて状態記憶手段４０２を備える。

【００４５】即ち、上記メモリカード４０１を構成するアクセス制限手段１０４は、例えば、当該メモリカードが外部接続機器に接続された際の通電時や上記スイッチ１０５の状態が変更された際等に、上記アクセス制限手段１０４を介して当該変更後のスイッチ１０５の状態を検出し、上記状態記憶手段４０２に記憶する。尚、上記状態記憶手段４０２は、例えば不揮発性メモリ等により構成されているため、例えばメモリカードに通電していない際でも記憶内容を保持可能である。

【００４６】続いて、アクセス制限手段１０４は再度所定のタイミングで上記スイッチの状態を再度検出し、上記状態記憶手段４０２に格納されている前回のスイッチの状態と比較する。ここで、前回のスイッチの状態が今回検出した状態と異なる場合、当該変更した後の上記スイッチの状態を、上記状態記憶手段４０２に記憶する。また、ここで例えば当該変更が、アクセス制限“あり”からアクセス制限“なし”への変更であった場合、上記アクセス制限手段１０４は、インターフェイス１０３を介して外部接続機器３０１に、ユーザへのパスワードの入力を求める旨の命令を送信する。

【００４７】上記パスワードの入力を求める旨の命令に対して、例えば上記外部接続機器３０１があらかじめ決められた手順にてユーザからのパスワードを受け付けると、当該パスワードを、インターフェイス１０３を介して上記アクセス制限手段１０４に通知する。

【００４８】上記パスワードを受信した上記アクセス制限手段１０４は、当該パスワードと例えば記憶手段１０

2にあらかじめ記憶されているパスワードとを比較し、一致すればその旨を上記アクセス手段１０６に通知する。

【００４９】上記パスワードが一致する旨を受信した上記アクセス手段１０６は、上記記憶手段１０２へのアクセスが可能となる。

【００５０】以上のように、上記スイッチの状態の変更を検知し、当該変更に基づいてアクセスの可不可を決定することで、例えばスイッチがオフの状態でメモリカードを紛失した場合、スイッチをオンにするのみでは記憶手段にアクセスできないため、メモリカードを紛失した場合などのアクセス制限（セキュリティ）も期待できる。また、通常のパスワードの要求と異なり、スイッチの状態が変更された場合のみパスワードが要求されるため、例えば電子商取引を複数回連続して行った場合等では、ユーザが連続してパスワードを入力するといった手間を省くことができる。

【００５１】尚、例えば上記アクセス制限手段１０４に、上記外部接続機器３０１に固有の番号等も格納することで、当該固有番号が変わった場合にもパスワードを求めるといったことが可能となる。

（実施の形態３）続いて、さらに複雑な構成を有するメモリカードへの対応について説明を行う。近年、メモリカードの様々な分野への応用が期待されている点は上述したとおりである。ここで、様々な分野への応用が期待されるがゆえに様々な情報を記憶する事が求められる。

【００５２】上記様々な情報とは、例えば、

・漏洩してもさほど問題にならない情報

・著作権を有するコンテンツ等、漏洩しても直ちに問題になるとは限らない情報

・クレジットカードの番号や電子商取引にて利用される電子マネー等、漏洩或いは改竄されることを絶対に防止しなければならない情報

等である。

【００５３】ところで、上記情報をそれぞれ同様に扱うことで問題が生じる場合がある。つまり、上記「漏洩してもさほど問題にならない情報」を記憶する場合、セキュリティ強度を高くし即ち認証や暗号化を行うことで、弊害としてユーザの入力の必要性や情報の記憶速度の低下などが発生し、意味なくユーザの利便性を損なってしまうのである。また、例えば音楽等のストリーミングコンテンツのセキュリティ強度を必要以上に高くしてしまうと、コンテンツを再生するたびに複雑な復号化処理が必要になり、即ちコンテンツの再生が間に合わないといった問題が起こってしまう。さらにＣＰＵなどにも高い能力が求められるため、メモリカードが高価になってしまい、複雑な処理により消費電力も増大するためにモバイル端末での利用が不利になってしまうのである。

【００５４】他方で、上記「漏洩或いは改竄されることを絶対に防止しなければならない情報」を記憶するには、セキュリティ強度を高くし、即ち十分な認証や暗号化を行う必要があるのである。

【００５５】上述したような種別の異なる情報を１枚のメモリカードに記憶するために、メモリカード内に複数の記憶領域を設けた多機能なメモリカードが提供されている。当該メモリカードは、記憶する情報に応じてセキュリティレベルの異なる記憶領域を使い分ける事で利便性及び耐タンパ性を兼ね備えている。

【００５６】ところが、このような複数の記憶領域を設けたメモリカードに上記実施の形態１にて述べたアクセス制限手段を適用すると問題が生じる。例えば、上記「漏洩或いは改竄されることを絶対に防止しなければならない情報」を知らぬ間に無線通信等にて読み出されないようにスイッチをＯＮ（又はＯＦＦ）することで、他の情報、例えば音楽コンテンツも利用できなくなってしまうのである。これでは、ユーザは、情報の安全と引き換えに利便性を失う事になってしまう。

【００５７】このため、本実施の形態３では、本発明の多機能なメモリカードへの対応方法について説明する。

【００５８】本実施の形態３におけるメモリカード５０１は、インターフェイス１０３、汎用メモリ部５１０、セキュアメモリ部５２０を備え、さらにアクセス制限手段１０４、スイッチ１０５を備えている。

【００５９】ここで、上記汎用メモリ部５１０は、アクセス手段１０６を構成するＣＰＵ５１１、ＲＡＭ５１２、ＲＯＭ５１３を備えており、さらに記憶手段５１５を備えている。上記ＣＰＵ５１１は、上記インターフェイス１０３を介して受信した、上記記憶手段５１５へのアクセス命令を解釈し、必要に応じて記憶手段１０２にアクセスを行う。尚、上記ＣＰＵ５１１は、ＲＡＭ５１２やＲＯＭ５１３より読み出されたプログラム等により後述する処理を行うが、詳細は適宜説明する。

【００６０】また、上記セキュアメモリ部５２０は、アクセス手段１０６を構成するＣＰＵ５２１、ＲＡＭ５２２、ＲＯＭ５２３、コプロセッサ５２４を備えており、さらに記憶手段５２５を備えている。上記ＣＰＵ５２１は、上記ＣＰＵ５１１より受信した、上記記憶手段５２５へのアクセス命令を解釈し、必要に応じて記憶手段１０２にアクセスを行う。尚、上記ＣＰＵ５２１は、ＲＡＭ５１２やＲＯＭ５１３より読み出されたプログラム等により後述する処理を行うが、詳細は適宜説明する。

【００６１】上記汎用メモリ部５１０における記憶手段５１５は、例えば認証不要領域と認証要領域により構成されており、上記ＣＰＵ５１１は、認証不要領域に対するアクセスについては全くアクセスを制限しない。つまり、例えば上記認証不要領域のアドレスを指定した読み出し命令を上記インターフェイス１０３を介して受信した場合、上記ＣＰＵ５１１は無条件で当該アドレスに対応するデータを読み出して、上記インターフェイス１０

3を介して送信するのである。これに対して、上記認証要領域に対するアクセスについては、上記CPU511はアクセス命令を送信した外部端末に対して、例えばパスワードを求める。当該パスワードを用いた認証に問題がなければ、上記CPU511は上記認証要領域に対してアクセスを行うのである。

【0062】ここで、例えば上記認証不要領域には、上述した「漏洩してもさほど問題にならない情報」が記憶される。また、認証要領域には、音楽コンテンツのような「漏洩しても直ちに問題になるとは限らない情報」が記憶される。

【0063】尚、上記セキュアメモリ部520を構成する記憶手段525へのアクセス命令を受信したCPU511は、例えばセキュアメッセージ等により高いセキュリティを保ちつつ上記CPU521と通信を行う。上記記憶手段525へのアクセス命令であるか否かは、例えば当該命令が電子商取引に関連する命令か否かで判断可能である。電子商取引に関連する命令である場合には、CPU511、又はCPU521の判断に基づいて自動的に記憶領域525にアクセスする事になる。

【0064】次に、上記セキュアメモリ部520における記憶手段525は、例えば上記「漏洩或いは改竄されることを絶対に防止しなければならない情報」が記憶される。ここで、上記CPU521は、上記CPU511より受信した記憶手段525へのアクセス命令に基づいて記憶手段525に対してアクセスを行う。尚、上記記憶手段525にアクセスするためには上記認証要領域へのアクセスよりも複雑な認証が行われる。また、上記記憶手段525内に記憶される情報はすべて暗号化されており高いセキュリティが保たれている。当該記憶手段525に記憶されている情報は、コプロセッサ524により復号化され、上記CPU511、インターフェイス103を介して外部接続機器に送信される。

【0065】さて、このような構成を有するメモリカードにおいて、アクセス制限手段502は、例えば上記CPU511とCPU521との接続ライン503を遮断すればよい。これにより、汎用メモリ部510は利用可能としながらも、セキュアメモリ部520へのアクセスを確実に防ぐ事ができ、即ちユーザはメモリカードの利便性を損なうことなく情報の安全性を手に入れる事ができる。当然、上記図2Aに示した方法によってセキュアメモリ部520を機能停止させてもよい。また、上記図2Bに示した方法により、接続ライン504を遮断する事により、記憶手段525へのアクセスを不能にしてもよい。

【0066】上述したのはセキュアメモリ部520の記憶手段525に対するアクセス制限であるが、例えば記憶手段515を構成する認証要領域と、上記CPU511との接続ライン505を遮断する事により、上記認証要領域へのアクセスを制限してもよい。

【0067】尚、上記セキュアメモリ部の一部は、例えばTRM(Tamper Resist Module)としてメモリカード内に設けられる場合がある。また、セキュアメモリ部にはセキュリティ強度の強い上記TRMと、当該TRMほどセキュリティ強度は強くないがメモリ容量が多い一般セキュアメモリ部とが設けられており、必要に応じて使い分けられる場合がある。

【0068】

【発明の効果】以上のように、メモリカード自身がスイッチの状態を判断し、さらにメモリカード自身が記憶手段へのアクセスを制限することで、例えば外部接続機器が悪意をもって記憶手段にアクセスした場合であっても、当該外部接続機器に依存することなくスイッチの状態に基づいて確実にアクセスを制限することが可能になる。これにより、近年増加しつつある、ネットワーク機能を利用した、悪意を持った外部からのアクセスを確実に防止することが可能となる。

【0069】また、ユーザが物理的にスイッチをオン・オフする構成とすることで、ユーザが気付かないうちに当該メモリカードに記憶しているデータが読み出されるという事態をメモリカードを外すことなく防止できるため、利便性を高めると共にユーザに安心感を与えることが可能になる。

【0070】また、スイッチの状態の変更を検知し、当該変更に基づいてアクセスの可不可を決定することで、メモリカードを紛失した場合などのアクセス制限(セキュリティ)が期待できる。また、通常のパスワードの要求と異なり、スイッチの状態が変更された場合のみパスワードが要求されるため、例えば電子商取引を複数回連続して行った場合等では、ユーザが連続してパスワードを入力するといった手間を省くことができる。

【0071】また、適所の接続ラインを物理的に遮断する事により、汎用メモリ部は利用可能としながらも、セキュアメモリ部へのアクセスを確実に防ぐ事ができ、即ちユーザはメモリカードの利便性を損なうことなく情報の安全性を手に入れる事ができる。

【図面の簡単な説明】

【図1】実施の形態1におけるメモリカードの概略機能ブロック図。

【図2】実施の形態1におけるメモリカードのハードウェアの概略図。

【図3】外部接続機器にメモリカードを挿入した際のイメージ図。

【図4】実施の形態2におけるメモリカードの概略機能ブロック図。

【図5】実施の形態3におけるメモリカードの概略機能ブロック図。

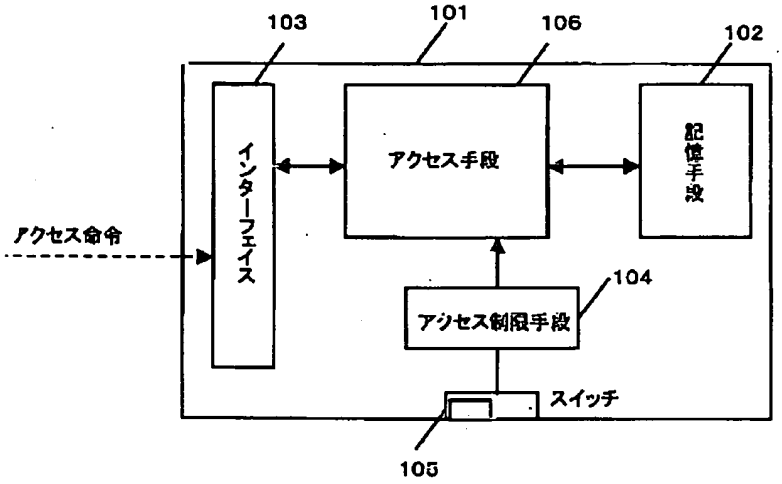
【符号の説明】

101 メモリカード

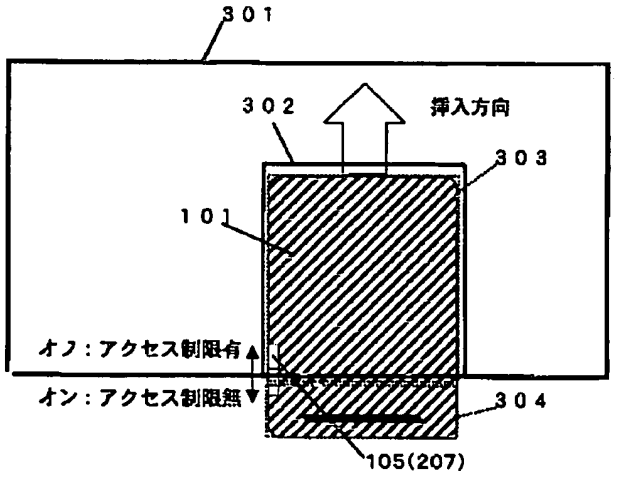
102 記憶手段

103　インターフェイス
104　アクセス制限手段
105　スイッチ
106　アクセス手段

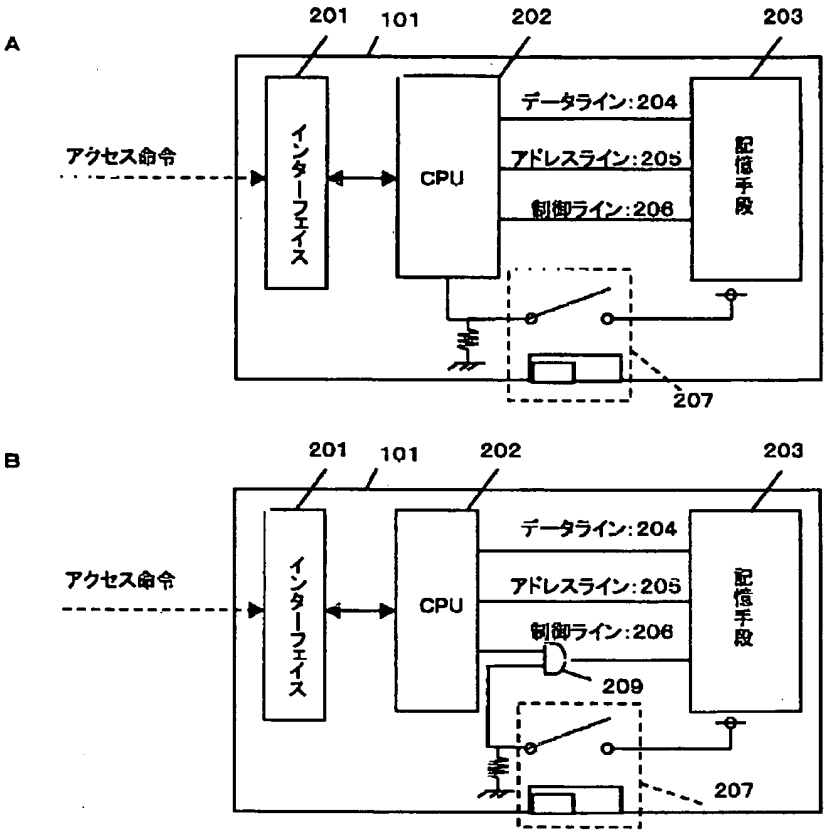
【図1】



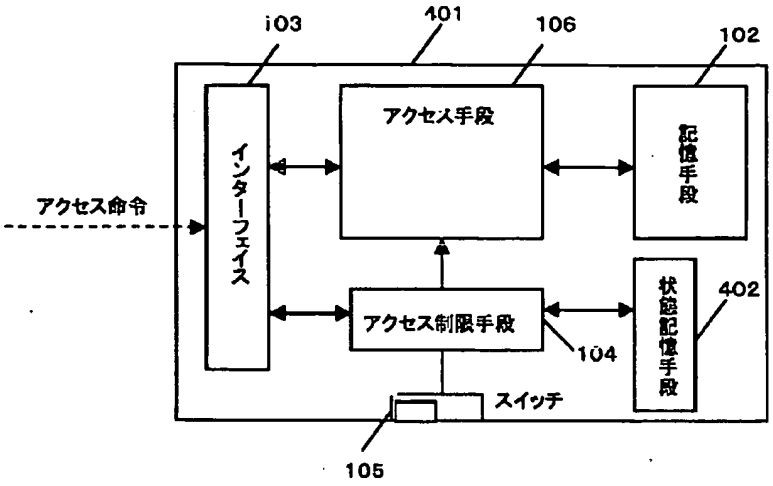
【図3】



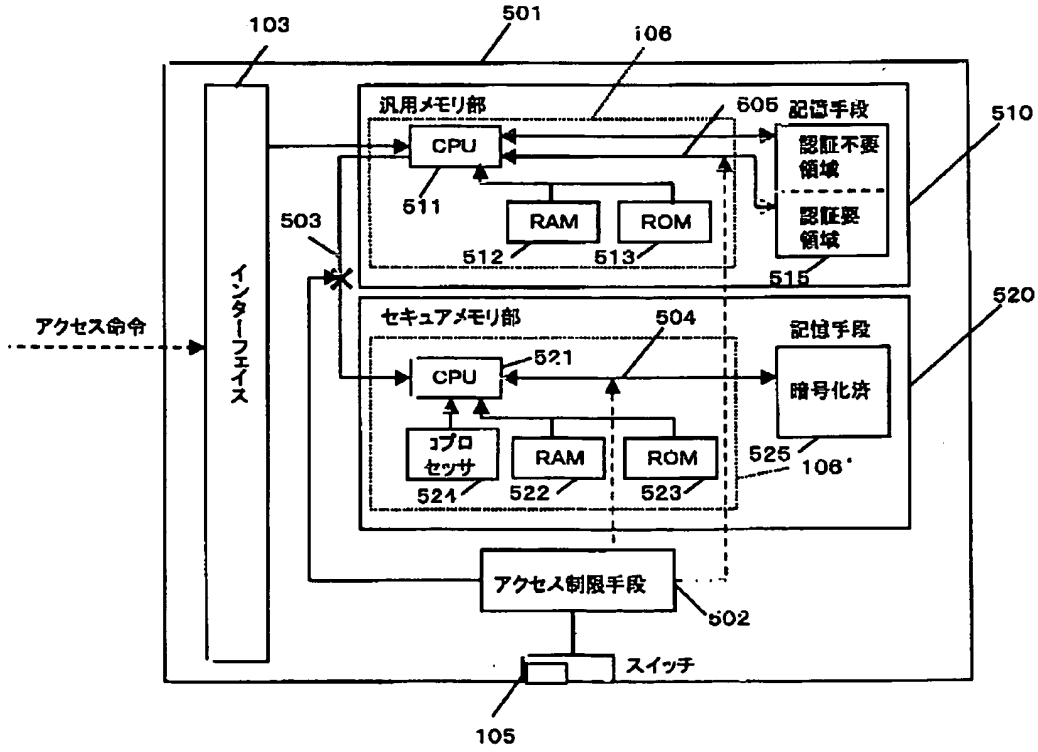
【図2】


A
201
101
202
203
アクセス命令
インターフェイス
CPU
データライン:204
アドレスライン:205
制御ライン:206
記憶手段
207
B
201
101
202
203
アクセス命令
インターフェイス
CPU
データライン:204
アドレスライン:205
制御ライン:206
209
記憶手段
207

【図4】


103
401
106
102
インターフェイス
アクセス手段
記憶手段
アクセス命令
アクセス制限手段
状態記憶手段
402
104
スイッチ
105

【図5】


103
501
106
汎用メモリ部
505
記憶手段
510
CPU
認証不要領域
認証要領域
511
RAM
ROM
503
512
513
515
520
セキュアメモリ部
504
記憶手段
アクセス命令
インターフェイス
CPU
521
暗号化済
コプロセッサ
RAM
ROM
525
106'
524
522
523
アクセス制限手段
502
スイッチ
105

フロントページの続き

(72)発明者　川野　眞二
東広島市鏡山３丁目10番18号　株式会社松下電器情報システム広島研究所内
(72)発明者　大関　秀夫
東広島市鏡山３丁目10番18号　株式会社松下電器情報システム広島研究所内
(72)発明者　江原　裕美
東広島市鏡山３丁目10番18号　株式会社松下電器情報システム広島研究所内

Fターム(参考)　5B017 AA02 AA03 BB03 CA14
5B035 AA13 BB09 BC00 CA05 CA11
CA38